



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|-----------------|-------------|----------------------|---------------------|------------------|
| 09/826,592 | 04/05/2001 | Radia J. Perlman | P4097 | 4832 |

25181 7590 11/10/2004

FOLEY HOAG, LLP
PATENT GROUP, WORLD TRADE CENTER WEST
155 SEAPORT BLVD
BOSTON, MA 02110

EXAMINER


POPHAM, JEFFREY D

ART UNIT PAPER NUMBER

2137

DATE MAILED: 11/10/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

| | | | |
|------------------------------|-------------------------------|--|--|
| Office Action Summary | Application No. 09/826,592 | Applicant(s) PERLMAN, RADIA J.  | |
| | Examiner Jeffrey D. Popham | Art Unit 2137 | |

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on ____.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-23 is/are pending in the application.
- 4a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) ____ is/are allowed.
- 6) ☐ Claim(s) 1-23 is/are rejected.
- 7) ☐ Claim(s) ____ is/are objected to.
- 8) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 05 April 2001 is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. ____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|--|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) Paper No(s)/Mail Date. ____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date <u>01022002, 07132001</u> . | 6) <input type="checkbox"/> Other: <u>1472</u> . |

Remarks

1. Claims 1-23 are pending.

Drawings

2. Figure 5 is objected to as being improperly labeled. Portion 52.2 is labeled as "First Certification Authority Serial No." in Figure 5, but is referred to as "a digest 52.2 of a public key of the CA 52" in the specification (Page 12, lines 2-3).

Claim Rejections - 35 USC § 101

3. Claim 20-21 rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Data structures not claimed as embodied in computer-readable media are descriptive material per se and are not statutory because they are not capable of causing functional change in the computer. Such claimed data structures do not define any structural and functional interrelationships between the data structure and other claimed aspects of the invention which permit the data structure's functionality to be realized. In contrast, a claimed computer-readable medium encoded with a data structure defines structural and functional interrelationships between the data structure and the computer software and hardware components which permit the data structure's functionality to be realized, and is thus statutory. A computer data signal with a computer program comprising program code is not within the bounds of statutory subject matter.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1-4, 6, 7, 9-11, 14, 15, and 18-23 are rejected under 35 U.S.C. 102(e) as being unpatentable over Van Oorschot et al. (U.S. 6,134,550).

Regarding Claim 1,

Van Oorschot et al. disclose a certification method, comprising the steps of: Acquiring a chain of linked certificates extending from a first entity, though at least one intermediate entity, to a second entity, the chain of linked certificates including a certificate signed by the intermediate entity vouching for predetermined information associated with the second entity (Column 5, lines 14-25); and generating, from the chain of linked certificates, a collapsed certificate (Column 5, lines 51-52) signed by the first entity vouching for the predetermined information associated with the second entity and including an identification of the at least one intermediate entity (Fig. 7a and Column 11, lines 8-23).

Regarding Claim 2,

Art Unit: 2137

The method of claim 1 wherein the predetermined information associated with the second entity includes a public key of the second entity (Column 11, lines 8-13).

Regarding Claim 3,

The method of claim 1 wherein each of the first entity and the at least one intermediate entity comprises a respective certification authority (Column 11, lines 8-23).

Regarding Claim 4,

The method of claim 3 wherein the identification of the at least one intermediate entity includes indications of a name and a key associated with the respective certification authority (Column 11, lines 30-37).

Regarding Claim 6,

The method of claim 3 wherein the collapsed certificate further includes an identification of the first entity (Column 11, lines 8-13).

Regarding Claim 7,

The method of claim 6 wherein the identification of the first entity includes indications of a name and a key associated with the respective certification authority (Fig. 7b and Column 11, lines 30-37).

Regarding Claim 9,

The method of claim 1 wherein the identification of the intermediate entity includes an indication of a name associated with the intermediate entity (Column 11, lines 8-23).

Regarding Claim 10,

The method of claim 1 wherein the first entity signs the collapsed certificate using a digital signature (Column 11, lines 30-37).

Regarding Claim 11,

The method of claim 1 further including the step of providing the collapsed certificate directly to an entity requesting the certificate (Column 5, lines 4-7).

Regarding Claim 22,

An apparatus for generating a collapsed certificate, comprising:
means for acquiring a chain of linked certificates extending from a first entity, through at least one intermediate entity, to a second entity, the chain of linked certificates including a certificate signed by the

intermediate entity vouching for predetermined information of the second entity (Column 5, lines 14-25); and generating, from the chain of linked certificates, a collapsed certificate (Column 5, lines 51-52) signed by the first entity vouching for the predetermined information associated with the second entity and including an identification of the at least one intermediate entity (Fig. 7a and Column 11, lines 8-23).

Regarding Claim 14,

Claim 14 is a system claim that is substantially equivalent to apparatus claim 22. Therefore, claim 14 is rejected under a similar rationale.

Art Unit: 2137

Regarding Claim 18,

Claim 18 is a computer program product including computer-readable medium claim that is substantially equivalent to apparatus claim 22. Therefore, claim 18 is rejected under a similar rationale.

Regarding Claim 20,

Claim 20 is a computer data signal that comprises program code claim that is substantially equivalent to apparatus claim 22. Therefore, claim 20 is rejected under a similar rationale.

Regarding Claim 23,

The apparatus of claim 22 further including means for providing the collapsed certificate directly to an entity requesting the certificate (Column 5, lines 4-7).

Regarding Claim 15,

Claim 15 is a system claim that is substantially equivalent to apparatus claim 23. Therefore, claim 15 is rejected under a similar rationale.

Regarding Claim 19,

Claim 19 is a computer program product including computer-readable medium claim that is substantially equivalent to apparatus claim 23. Therefore, claim 19 is rejected under a similar rationale.

Regarding Claim 21,

Claim 21 is a computer data signal that comprises program code claim that is substantially equivalent to apparatus claim 23. Therefore, claim 21 is rejected under the same rationale.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claims 12, 13, 16, and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Van Oorschot et al. (U.S. 6,134,550) in view of Hind et al. (U.S. 6,772,331).

Regarding Claim 16,

A system for determining whether access to a first node in a computer network should be granted to a client at a second node in the network in response to a request for access to the first node by the client, the system comprising (Column 11, lines 8-23):

a server operative to:

receive the request for access to the first node from the client at the second node, the request including a collapsed certificate (Column 5, lines 51-52) signed by a first certification authority vouching for predetermined

information of the client and including an identification of an intermediate certification authority that vouches for the client's predetermined information (Fig. 7a and Column 11, lines 8-23);

determine whether the identification of the intermediate certification authority matches an identifier contained in a certificate revocation list (Column 8, lines 24-35); and

in the event the identification of the intermediate certification authority matches an identifier contained at the first node that a certificate for the intermediate certification authority has been revoked and deny the client access to the first node (Column 8, lines 14-23).

Van Oorschot et al. fail to disclose the fact that the first node is attempting to access a resource on the second node.

Hind et al., however, disclose the fact that the first node is attempting to access a resource on the second node (Column 12, lines 20-29 and Column 12, lines 43-53). This new system would be the system of Van Oorschot et al. used to access remote resources, as in Hind et al.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention that the certificate authentication method of Van Oorschot et al. could be used to authenticate users who access resources every day. One of ordinary skill in the art would be motivated to use the certificate authentication method described in Van Oorschot et al.

to access resources across a network because professionals utilize remote resources all the time, whether it be with a cell phone, pager, or computer (Column 1, lines 29-37).

Regarding Claim 12,

Claim 12 is a method claim that is substantially equivalent to apparatus claim 16. Therefore, claim 12 is rejected under a similar rationale.

Regarding Claim 17,

Van Oorschot et al. disclose the method of claim 16 wherein the server is further operative to verify the authenticity of the request using a digital signature of the first certification authority (Column 11, lines 8-13).

Regarding Claim 13,

Claim 13 is a method claim that is substantially equivalent to apparatus claim 17. Therefore, claim 13 is rejected under a similar rationale.

8. Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Van Oorschot et al. (U.S. 6,134,550) in view of Vu et al. (U.S. 6,557,104).

Van Oorschot et al. fail to disclose that the indication of the key associated with the respective certification authority comprises a digest of the key.

Vu et al., however, disclose this method of key storage and transfer (Column 6, lines 36-53). This new system would be the system of Van Oorschot

et al. with the digest of the certification authority's key from Vu et al. added into the collapsed certificate.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to use a digest of the key from Vu et al. for verification so as to provide more security, thus making the authentication process of Van Oorschot et al. better. One of ordinary skill in the art would be motivated to use a digest of the key for verification to add more security to prevent unauthorized access to the system (Column 6, lines 51-53).

9. Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over Van Oorschot et al. (U.S. 6,134,550) in view of Hallin et al. (U.S. 6,754,661).

Van Oorschot et al. fail to disclose the fact that the collapsed certificate further includes a digest of the collapsed certificate.

Hallin et al., however, disclose this method of a digest of the collapsed certificate being stored in the collapsed certificate itself (Column 2, lines 63-66). This new system would be the system of Van Oorschot et al. with the digest of the certificate from Hallin et al. added into the collapsed certificate.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to add a digest of the certificate from Hallin et al. to the certificate itself so as to provide more security in the system of Van Oorschot et al. One of ordinary skill in the art would be motivated to use a digest of the

Art Unit: 2137

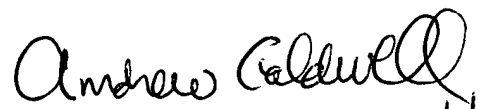
certificate in the certificate itself in order to ensure that the certificate has not been altered or forged (Hallin et al., Column 2, lines 63-66).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffrey D. Popham whose telephone number is (571)-272-3860. The examiner can normally be reached on M-F 8-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571)-272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).


Andrew Caldwell